

Quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations

YAN Feng-Li¹, GAO Ting², LI You-Cheng¹

¹ *College of Physics Science and Information Engineering,
Hebei Normal University, Shijiazhuang 050016, China*

² *College of Mathematics and Information Science,
Hebei Normal University, Shijiazhuang 050016, China*

(Dated: February 3, 2008)

We propose a scheme of quantum secret sharing between Alices' group and Bobs' group with single photons and unitary transformations. In the protocol, one member in Alices' group prepares a sequence of single photons in one of four different states, while other members directly encode their information on the sequence of single photons via unitary operations, after that the last member sends the sequence of single photons to Bobs' group. Then Bobs except for the last one do work similarly. Finally last member in Bobs' group measures the qubits. If Alices and Bobs guaranteed the security of quantum channel by some tests, then the qubit states sent by last member of Alices' group can be used as key bits for secret sharing. It is shown that this scheme is safe.

PACS numbers: 03.67.Dd; 03.67.Hk

Quantum cryptography or quantum key distribution is a remarkable application of quantum information. It has attracted widespread attention since the seminal work on quantum key distribution by Bennett and Brassard [1] and Ekert [2]. So far there are many quantum key distribution theoretical protocols [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18]. Some of them were demonstrated in the laboratory and will be used in the future secret communications. With quantum mechanics, other cryptographic tasks can be realized, such as quantum secure direct communication [19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36] and quantum secret sharing (QSS) [37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57].

Assume that there are a manager Alice, and her agents Bob and Charlie, who are at remote places. One of the agents, Bob or Charlie, is not entirely trusted by Alice, and unfortunately she does not know who is the honest one. However Alice knows that if Bob and Charlie cooperate, the honest one will keep the dishonest one from doing anything wrong. By means of the secret sharing Alice can instruct Bob and Charlie to complete a task safely. The idea of secret sharing is that a secret of Alice, is shared between her agents, Bob and Charlie, in such a way that it can only be reconstructed if both collaborate. However, as a matter of fact, there is not any classical mean to establish a secret sharing between Alice and two distant agents Bob and Charlie. Amazingly, the principle of quantum mechanics has now provided the foundation stone to QSS referring to the implementation of the secret sharing task. The first QSS protocol of quantum secret sharing [37] was put forward by Hillery, Bužek and Berthiaume using entangled three-photon Greenberger-Horne-Zeilinger (GHZ) states. Xiao et al [38] reformulated the protocol [37] into arbitrary number party case. Karlsson et al [39] realized secret sharing as in Ref. [37] with two-particle quantum entanglement. They also dis-

cussed how to detect eavesdropping, or how to detect a dishonest party in the protocols. Furthermore, the concept of quantum sharing of classical secrets has also been generalized to the sharing of secret quantum information, which is often called quantum state sharing [48, 49]. In a more general case, notably for secure key management, a *t-out-of-n* protocol (or (t, n) -threshold scheme) with $1 \leq t \leq n$ spreads a secret to n participants in a way that any t participants can reconstruct it [50]. Recently, Lance et al reported an experimental demonstration of a (2,3) threshold QSS protocol [51].

Most of the existing QSS protocols use entangled states [37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47]. However it is believed that implementing such multiparty secret sharing tasks is not always so easy, as the efficiency of preparing entangled states is very low [58, 59], at the same time the efficiency of the existing QSS protocols using quantum entanglement can only approach 50%. Recently, a scheme for quantum secret sharing without entanglement has been proposed by Guo and Guo [52]. They presented an idea to directly encode the qubit of quantum key distribution and accomplish one splitting a message into many parts to achieve one-to-multiparty secret sharing only by product states. The theoretical efficiency is doubled to approach 100%. Deng et al also presented a one-to-multiparty secret sharing by using single photons [53]. Zhang et al proposed an QSS protocol by using single photons and unitary transformations [54, 55, 56].

Signatures on documents, authentications, encryptions, and decryptions are often needed by more than one person, especially by all persons of two groups in a trade. Therefore, it is needed to share a secret between many parties and many parties. That is, it is required the secret message shared by two groups, in such a way that neither any subset of each group nor the union of a subset of group 1 and a subset of group 2 can extract the secret message, but the entire group 1 or group 2 can. More

recently, we proposed a quantum secret sharing scheme employing two conjugate bases, i.e. four states, of single qubits to achieve the secret sharing between multiparty and multiparty with a sequence of single photons [57]. The weakness of our protocol was pointed out by Deng et al [60] and Li et al [61], they also gave a little modification to avoid the flaw. We have avoided the flaw pointed out in Ref. [61] with a little improvement of our protocol [62]. Another QSS protocol between multiparty and multiparty using three rather than two conjugate bases was suggested by us [63].

In present Letter, we will combine the protocol of Zhang's in Ref. [54] and ours [57, 62] to figure out a scheme of quantum secret sharing between multiparty and multiparty with single photons and unitary transformations. The security of this protocol is discussed.

Let us suppose that group 1 and group 2 are located in different places, and there are members Alice 1, Alice 2, \dots , Alice m , and Bob 1, Bob 2, \dots , Bob n in group 1, and group 2 respectively. Here $m \geq 2$ and $n \geq 2$. Group 1 and group 2 want quantum secret sharing such that neither part of each group nor the combination of a part of group 1 and a part of group 2 knows the key, but only all members of each group can collaborate to determine what the string (key) is. A protocol employing two conjugate bases going as follows will meet the goal of quantum secret sharing.

M1. Alice 1 generates two random classical bit strings $A_1 = \{a_1^1, a_2^1, \dots, a_N^1\}$ and $B_1 = \{b_1^1, b_2^1, \dots, b_N^1\}$, where a_k^1 and b_k^1 are uniformly taken from $\{0, 1\}$. Based on these two strings A_1 and B_1 she then makes a block of N qubits (single photons),

$$|\Psi^1\rangle = \otimes_{k=1}^N |\psi_{a_k^1 b_k^1}\rangle, \quad (1)$$

where a_k^1 is the k th bit of A_1 (and similar for B_1), each qubit $|\psi_{a_k^1 b_k^1}\rangle$ is in one of the four states

$$|\psi_{00}\rangle = |0\rangle, \quad (2)$$

$$|\psi_{10}\rangle = |1\rangle, \quad (3)$$

$$|\psi_{01}\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad (4)$$

$$|\psi_{11}\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (5)$$

The basis is determined by the value of b_k^1 . If b_k^1 is 0 then a_k^1 is encoded in the Z basis $|0\rangle, |1\rangle$; if b_k^1 is 1 then a_k^1 is encoded in the X basis $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. As the four states are not all mutually orthogonal, so there is no measurement which can distinguish between all of them with certainty. Alice 1 then delivers $|\Psi^1\rangle$ to Alice 2 over their public quantum communication channel.

M2. When Alice i ($i = 2, 3, \dots, m$) receives N signals delivered by Alice $i-1$ she use a special filter to prevent the invisible photons from entering the operation system [56, 65]. Then she chooses randomly a sufficiently enough subset of photons as the samples for eavesdropping check.

First, let sample photon signals go to a photon number splitter (PNS: 50/50), and then measures each signal in the measurement basis (MB) Z , or X choosing randomly [60]. Evidently if more than two photons in one signal are measured, then Alice i will abort the communication. Moreover, she analyzes the error rate ε_s of the samples by means that she requires Alice 1, Alice 2, \dots , Alice $i-1$ to tell her the original states of the samples and the operations implemented by them. If the error rate is reasonably lower than the threshold ε_t , Alice i goes ahead, otherwise she aborts it.

M3. Alice i ($i = 2, 3, \dots, m$) generates a quaternary string $A_i = \{a_1^i, a_2^i, \dots, a_N^i\}$ and a binary string $B_i = \{b_1^i, b_2^i, \dots, b_N^i\}$, where a_k^i and b_k^i are uniformly chosen from $\{0, 1, 2, 3\}$ and $\{0, 1\}$, respectively. For each $|\psi_{a_k^{i-1} b_k^{i-1}}\rangle$ of the N qubit state $|\Psi^{i-1}\rangle = \otimes_{k=1}^N |\psi_{a_k^{i-1} b_k^{i-1}}\rangle$, she implements the operation $\sigma_0, \sigma_1, \sigma_2$ or σ_3 on it depending on the corresponding a_k^i of A_i is 0, 1, 2 or 3, respectively. At the same time she operates the qubit with I or a Hadamard operator H according to the bit b_k^i in B_i is 0 or 1, respectively. Here

$$\begin{aligned} \sigma_0 &= I = |0\rangle\langle 0| + |1\rangle\langle 1|, \\ \sigma_1 &= i\sigma_y = -|1\rangle\langle 0| + |0\rangle\langle 1|, \\ \sigma_2 &= \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \\ \sigma_3 &= \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \\ H &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|. \end{aligned} \quad (6)$$

These unitary operations made by Alice i are equal to the encryption on the states of single photons. The resulting state of this qubit is denoted by $|\psi_{a_k^i b_k^i}\rangle$.

M4. Alice i sends the photons (N qubit state $|\Psi^i\rangle = \otimes_{k=1}^N |\psi_{a_k^i b_k^i}\rangle$) to Alice $i+1$ ($i = 2, 3, \dots, m-1$). Alice m sends N -qubit state $|\Psi^m\rangle = \otimes_{k=1}^N |\psi_{a_k^m b_k^m}\rangle$ to Bob 1.

M5. When Bob j ($j = 1, 2, \dots, n-1$) has received string of N qubits, he does work similarly. First he makes eavesdropping check using the method Alice i used. If the error rate of the samples is higher than a threshold then he aborts the quantum communication. Otherwise he creates a quaternary string $C_j = \{c_1^j, c_2^j, \dots, c_N^j\}$ and a binary string $D_j = \{d_1^j, d_2^j, \dots, d_N^j\}$. Depending on the values of c_k^j and d_k^j he makes operations on the qubits just like Alice i does. That is, he applies the operation $\sigma_0, \sigma_1, \sigma_2$ or σ_3 on it depending on the corresponding c_k^j of C_j is 0, 1, 2 or 3, respectively; and he implements the operation I or a Hadamard operator H on the qubit according to the bit d_k^j in D_j is 0 or 1, respectively.

M6. Bob n first randomly and independently chooses sufficient samples to make measurement in MB Z , or X randomly. Then he asks Alice 1, Alice 2, \dots , Alice m , and Bob 1, Bob 2, \dots , Bob $n-1$ to announce publicly the $a_s^i, b_s^i, c_s^j, d_s^j$ of the samples in a random sequential order. After that he checks the error rate of the samples measured in the MB Z or X according to the XOR results of the corresponding sample bits in the strings $B_1, B_2, \dots, B_m, D_1, D_2, \dots, D_{n-1}$. If the error rate is

higher than the threshold ε_t , Bob n aborts it, otherwise they go to the next step.

M7. All members in group 1 and group 2 publicly announce the strings B_1, B_2, \dots, B_m and D_1, D_2, \dots, D_{n-1} . Bob n measures each of their qubits with the MB Z or X according to the XOR (i.e., \oplus) results of the corresponding bits in the strings $B_1, B_2, \dots, B_m, D_1, D_2, \dots, D_{n-1}$.

M8. Two groups make the error rate analysis of the transmission between the two groups. To this end, it requires that all Alices and all Bobs publicly announce a_s^i and the measurement results of the sample qubits chosen randomly, and analyze the error rates of the samples. If the channel is secure, the qubit states sent by Alice m can be used as key bits for secret sharing, otherwise they discard the results obtained and retry the quantum communication from the beginning.

Now we discuss the security of this quantum secret sharing protocol between m parties and n parties with single photons and unitary transformations. Obviously, the test in M2 and M5 can nullify the attack with invisible photons [65] and the Trojan horse attack [60]. The checking procedure in M5 can avoid the attack with single photons and attack with EPR pairs [62]. The fake-signal attack with EPR pairs can be detected by the operations in M3 and the check in M2 and M5 [62]. So we can believe the security of the protocol without question.

We should point out that the above protocol can be generalized to the situation where three conjugate bases, or six states are employed [63].

In summary, we propose a scheme for quantum secret sharing between multi-party and multi-party with single photons and unitary transformations, where no

entanglement is employed. In the protocol, Alice 1 prepares a sequence of single photons in one of four different states according to her two random classical strings, other Alice i ($2 \leq i \leq m$) directly encodes her information strings on the resulting sequence of Alice ($i-1$) via unitary operations, after that Alice m sends the sequence of single photons to Bob 1. Bob l ($l = 1, 2, \dots, n-1$) does work similar to Alice i . Finally Bob n measures the qubits. If Alices and Bobs guarantee the security of quantum channel by some tests, then the qubit states sent by Alice m can be used as key bits for secret sharing. Any subset of all Alices or all Bobs can not extract secret information, but the entire set of all Alices and the entire set of all Bobs can. It is shown that this scheme is in safety. As entanglement, especially the inaccessible multi-party entangled state, is not necessary in the present quantum secret sharing protocol between m -party and n -party, it may be more applicable when the numbers m and n of the parties of secret sharing are large. This protocol is feasible with present-day technique.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant No: 10671054, Hebei Natural Science Foundation of China under Grant Nos: A2005000140, 07M006, and the Key Project of Science and Technology Research of Education Ministry of China under Grant No: 207011.

-
- [1] C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India, (IEEE, New York, 1984), pp. 175-179.
 - [2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
 - [3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
 - [4] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
 - [5] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
 - [6] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
 - [7] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).
 - [8] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
 - [9] W. Y. Hwang, I. G. Koh, and Y. D. Han, Phys. Lett. A **244**, 489 (1998).
 - [10] A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000).
 - [11] A. Cabello, Phys. Rev. A **61**, 052312 (2000).
 - [12] G. L. Long and X. S. Liu, Phys. Rev. A **65**, 032302 (2002).
 - [13] P. Xue, C. F. Li, and G. C. Guo, Phys. Rev. A **65**, 022317 (2002).
 - [14] S. J. D. Phoenix, S. M. Barnett, P. D. Townsend, and K. J. Blow, J. Modern Optics **42**, 1155 (1995).
 - [15] D. Song, Phys. Rev. A **69**, 034301 (2004).
 - [16] X. B. Wang, Phys. Rev. Lett. **92**, 077902 (2004).
 - [17] X. B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Phys. Rep. **448**, 1 (2007).
 - [18] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden Rev. Mod. Phys. **74** 145 (2002).
 - [19] G.L. Long, F. G. Deng, C. Wang, X. H. Li, Front. Phys. China, **2**, 251 (2007).
 - [20] K. Shimizu and N. Imoto, Phys. Rev. A **60**, 157 (1999).
 - [21] K. Shimizu and N. Imoto, Phys. Rev. A **62**, 054303 (2000).
 - [22] A. Beige *et al*, Acta Phys. Pol. A **101**, 357 (2002).
 - [23] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).
 - [24] Q. Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003).
 - [25] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
 - [26] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).
 - [27] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).
 - [28] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, Phys. Rev. A **71**, 044305 (2005).
 - [29] Q. Y. Cai and B. W. Li, Chin. Phys. Lett. **21**, 601 (2004).
 - [30] Q. Y. Cai and B. W. Li, Phys. Rev. A **69**, 054301 (2004).

- [31] Z. J. Zhang, Z. X. Man and Y. Li, Phys. Lett. A **333**, 46 (2004).
- [32] Z. J. Zhang, Z. X. Man and Y. Li, Phys. Lett. A **341**, 55 (2004).
- [33] A. D. Zhu, Y. Xia, Q. B. Fan and S. Zhang, Phys. Rev. A **73**, 022388 (2006).
- [34] H. J. Cao and H. S. Song, Chin. Phys. Lett., **23**, 290 (2006).
- [35] F. L. Yan and X. Q. Zhang, Euro. Phys. J. B **41**, 75 (2004).
- [36] T. Gao, F. L. Yan, and Z. X. Wang, J. Phys. A: **38**, 5761 (2005).
- [37] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
- [38] L. Xiao, G. L. Long, F. G. Deng, and J. W. Pan, Phys. Rev. A **69**, 052307 (2004).
- [39] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
- [40] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
- [41] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
- [42] A. C. A. Nascimento, J. M. Quade, and H. Imai, Phys. Rev. A **64**, 042311 (2001).
- [43] R. Cleve, D. Gottesman, and H. K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
- [44] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, Phys. Rev. A **65**, 042320 (2002).
- [45] F. G. Deng, G.L. Long and H. Y. Zhou, Phys. Lett. A, **340**, 43 (2005).
- [46] Z. J. Zhang and Z. X. Man, Phys. Rev. A **72**, 022303 (2005).
- [47] Z. J. Zhang, J. Yang, Z. X. Man and Y. Li, Eur. Phys. J. D **33**, 133 (2005).
- [48] F. G. Deng, et al Phys. Rev. A **72**, 044301 (2005).
- [49] F. G. Deng, C. Y. Li, Y. S. Li, H. Y. Zhou and Y. Wang, Phys. Rev. A **72**, 022338 (2005).
- [50] Y. Tokunaga, T. Okamoto, and N. Imoto, Phys. Rev. A **71**, 012314 (2005).
- [51] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
- [52] G. P. Guo and G. C. Guo, Phys. Lett. A **310**, 247 (2003).
- [53] F. G. Deng, H. Y. Zhou, and G.L. Long, Phys. Lett. A, **337**, 329 (2005).
- [54] Z. J. Zhang, Y. Li and Z. X. Man, Phys. Rev. A **71**, 044301 (2005).
- [55] F. G. Deng, X. H. Li, H. Y. Zhou and Z. J. Zhang, Phys. Rev. A **72**, 044302 (2005).
- [56] F. G. Deng, X. H. Li, H. Y. Zhou and Z. J. Zhang, Phys. Rev. A **73**, 049901 (2006).
- [57] F. L. Yan and T. Gao, Phys. Rev. A **72**, 012304 (2005).
- [58] D. Bouwmeester, J. W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999).
- [59] J. W. Pan, M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **86**, 4435 (2001).
- [60] F. G. Deng, F. L. Yan, X. H. Li, C. Y. Li, H. Y. Zhou and T. Gao, arXiv: quant-ph/0508171.
- [61] C. M. Li, C. C. Chang and T. Hwang, Phys. Rev. A, **73**, 016301 (2006).
- [62] F. L. Yan, T. Gao, and Y. C. Li, Science in China Series G, **50**, 572 (2007).
- [63] T. Gao and F. L. Yan, arXiv: quant-ph/0601111.
- [64] F. G. Deng, X. H. Li, P. Chen, C. Y. Li, and H. Y. Zhou, arXiv: quant-ph/0604060.
- [65] Q. Y. Cai, Phys. Lett. A **351**, 23 (2006).
- [66] G. P. Guo and G. C. Guo, Quant. Infor. Comp. **3**, 627 (2003).
- [67] C. H. Bennett, G. Brassard, S. Briedbart and S. Wiesner, IBM Tech. Disclosure Bulletin **26**, 4363 (1984).
- [68] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
- [69] H. -K. Lo, Quant. Info. Comp. **1**, 81 (2001).